PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

pre-authenticate and public key SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **pre authenticate** and **public key**

Found **37,229** of **201,062**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □ ▭ ▬ ■ ■

1 Mobile Code and Distributed Systems: The performance of public key-enabled kerberos authentication in mobile computing applications

Alan Harbitter, Daniel A. Menascé

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

Full text available: pdf(419.31 KB) Additional Information: full citation, abstract, references, citings, index terms

Authenticating mobile computing users can require a significant amount of processing and communications resources-particularly when protocols based on public key encryption are invoked. These resource requirements can result in unacceptable response times for the user. In this paper, we analyze adaptations of the public key-enabled Kerberos network authentication protocol to a mobile platform by measuring the service time of a "skeleton" implementation and constructing a closed queuing network m ...

Keywords: authentication, kerberos, mobile computing, performance modeling, proxy servers, public key cryptography

2 Cryptology I: Authenticated group key agreement with admission control

Wen Hailong, Gu Dawu

November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**

Publisher: ACM Press

Full text available: pdf(408.18 KB) Additional Information: full citation, abstract, references, index terms

In this paper we present an authenticated group key agreement scheme with admission control for dynamic peer groups. Admission control is a necessary part of group communication. The scheme uses secret sharing to achieve integration of admission control and key agreement and addresses the pre-requisite for key management. Identity-based cryptosystems are used for mutual authentication and key agreement, and it avoids bandwidth consuming and expensive computation arising from certificates in PKI.

Keywords: admission control, group key agreement, identity-based cryptosystem, secret sharing

3 A methodology for analyzing the performance of authentication protocols

Alan Harbitter, Daniel A. Menascé

November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 4

Publisher: ACM Press

Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, index terms

Performance, in terms of user response time and the consumption of processing and communications resources, is an important factor to be considered when designing authentication protocols. The mix of public key and secret key encryption algorithms typically included in these protocols makes it difficult to model performance using conventional analytical methods. In this article, we develop a validated modeling methodology to be used for analyzing authentication protocol features, and we use two ...

Keywords: Authentication, Kerberos, mobile computing, performance modeling, proxy servers, public key cryptography

4 Security: Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks
Mohamed Kassab, Abdelfettah Belghith, Jean-Marie Bonnin, Sahbi Sassi
October 2005 **Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling WMuNeP '05**
Publisher: ACM Press
Full text available: pdf(398.42 KB) Additional Information: full citation, abstract, references, index terms

Recently, user mobility in wireless data networks is increasing because of the popularity of portable devices and the desire for voice and multimedia applications. These applications, however, require fast handoffs among base stations to maintain the quality of the connections. Re-authentication during handoff procedures causes a long handoff latency which affects the flow and service quality especially for multimedia applications. Therefore minimizing re-authentication latency is crucial in ord ...

Keywords: IAPP, IEEE 802.11i, WiFi, handover, pre-authentication, re-authentication

5 Location-based techniques: Integrity regions: authentication through presence in wireless networks
Srdjan Čapkun, Mario Čagalj
September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**
Publisher: ACM Press
Full text available: pdf(193.63 KB) Additional Information: full citation, abstract, references, index terms

We introduce *Integrity (I) regions*, a novel security primitive that enables message authentication in wireless networks without the use of pre-established or pre-certified keys. Integrity regions are based on the verification of entity proximity through time-of-arrival ranging techniques. We demonstrate how I-regions can be efficiently implemented with ultrasonic ranging, in spite of the fact that ultrasound ranging techniques are vulnerable to distance enlargement and reduction attacks. ...

Keywords: authentication, distance bounding, key establishment, wireless networks

6 DoS and authentication in wireless public access networks
Daniel B. Faria, David R. Cheriton
September 2002 **Proceedings of the 3rd ACM workshop on Wireless security WiSE '02**
Publisher: ACM Press
Full text available: pdf(272.24 KB) Additional Information: full citation, abstract, references, citings, index terms

As WEP has been shown to be vulnerable to multiple attacks, a huge effort has been placed on specifying an access control mechanism to be used in wireless installations. However, properties of the wireless environment have been exploited to perform multiple DoS attacks against current solutions, such as 802.11/802.1X. In this paper we discuss the main wireless idiosyncrasies and the need for taking them into account when designing an access control mechanism that can be used in both wireless and ...

Keywords: DoS, security, wireless networks

7 Wireless network security II: Authentication protocols for ad hoc networks: taxonomy and research issues
Nidal Aboudagga, Mohamed Tamer Refaei, Mohamed Eltoweissy, Luiz A. DaSilva, Jean-Jacques Quisquater
October 2005 **Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks Q2SWinet '05**
Publisher: ACM Press
Full text available: Additional Information:

pdf(314.61 KB) full citation, abstract, references, index terms

Ad hoc networks, such as sensor and mobile ad hoc networks, must overcome a myriad of security challenges to realize their potential in both civil and military applications. Typically, ad hoc networks are deployed in un-trusted environments. Consequently, authentication is a precursor to any secure interactions in these networks. Recently, numerous authentication protocols have been proposed for ad hoc networks. To date, there is no common framework to evaluate these protocols. Towards developin ...

Keywords: ad hoc networks, authentication, credentials, identity verification, network security, protocol taxonomy

8 Mobility, roaming, and handoff: Fast authentication methods for handovers between IEEE 802.11 wireless LANs
M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, P. Schoo
October 2004 **Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '04**
Publisher: ACM Press
Full text available: pdf(257.82 KB) Additional Information: full citation, abstract, references, index terms, review

Improving authentication delay is a key issue for achieving seamless handovers across networks and domains. This paper presents an overview of fast authentication methods when roaming within or across IEEE 802.11 Wireless-LANs. Besides this overview, the paper analyses the applicability of IEEE 802.11f and Seamoby solutions to enable fast authentication for inter-domain handovers. The paper proposes a number of possible changes to these solutions (typically in terms of network architectures a ...

Keywords: WLAN, authentication, handover, inter/intra-domain, seamless

9 Cryptographic tools: The dual receiver cryptosystem and its applications
Theodore Diament, Homin K. Lee, Angelos D. Keromytis, Moti Yung
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**
Publisher: ACM Press
Full text available: pdf(329.14 KB) Additional Information: full citation, abstract, references, citings, index terms

We put forth the notion of a dual receiver cryptosystem and implement it based on bilinear pairings over certain elliptic curve groups. The cryptosystem is simple and efficient yet powerful, as it solves two problems of practical importance whose solutions have proven to be elusive before:(1) A provably secure "combined" public-key cryptosystem (with a single secret key per user in space-limited environment) where the key is used for both decryption and signing and where encryption can be esc ...

Keywords: digital signature, elliptic curves, key escrow, pairing-based cryptography, public key, puzzles, useful secure computation

10 Anonymity systems & formal method: A *k*-anonymous communication protocol for overlay networks
Pan Wang, Peng Ning, Douglas S. Reeves
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(456.01 KB) Additional Information: full citation, abstract, references, index terms

Anonymity is increasingly important for network applications concerning about censorship and privacy. The existing anonymous communication protocols generally stem from mixnet and DC-net. They either cannot provide provable anonymity or suffer from transmission collision. In this paper, we introduce a novel approach which takes advantage of hierarchical ring structure and mix technique. This proposed protocol is collision free and provides provable *k*-anonymity for both the sender and the ...

Keywords: anonymity, overlay networks, security

11 Fast Handoff in Mobile Virtual Private Networks

Jyh-Cheng Chen, Jui-Chi Liang, Siao-Ting Wang, Shin-Ying Pan, Yin-Shin Chen, Ying-Yu Chen
June 2006 **Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks WOWMOM '06**
Publisher: IEEE Computer Society
Full text available: pdf(587.83 KB) Additional Information: full citation, abstract, index terms

This paper presents the dynamic external Home Agent (x-HA) assignment, fast authentication, and preauthentication in mobile Virtual Private Networks (VPNs). The proposed architecture is based on the mobile VPN proposed by the IETF, which adopts Mobile IP and IPsec. The IETF solution, however, leads to two questions: where should we put the x-HA and how should we trust the x-HA? We propose to assign the x-HA dynamically so the handoff latency and end-to-end latency could be reduced significantly. ...

12 Response to "Problems with DCE security services"
Walter Tuvell
April 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 2
Publisher: ACM Press
Full text available: pdf(1.01 MB) Additional Information: full citation, index terms

13 Wireless hotspots: current challenges and future directions
Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl
June 2005 **Mobile Networks and Applications**, Volume 10 Issue 3
Publisher: Kluwer Academic Publishers
Full text available: pdf(780.01 KB) Additional Information: full citation, abstract, references, index terms

In recent years, wireless Interact service providers (WISPs) have established Wi-Fi hotspots in increasing numbers at public venues, providing local coverage to traveling users and empowering them with the ability to access email, Web, and other Internet applications on the move. In this paper, we observe that while the mobile computing landscape has changed both in terms of number and type of hotspot venues, there are several technological and deployment challenges remaining before hotspots can ...

Keywords: deployment, performance

14 Vision & challenges: Wireless hotspots: current challenges and future directions
Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl
September 2003 **Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '03**
Publisher: ACM Press
Full text available: pdf(117.89 KB) Additional Information: full citation, abstract, references, citings, index terms

In recent years, wireless Internet service providers (WISPs) have established Wi-Fi hotspots in increasing numbers at public venues, providing local coverage to traveling users and empowering them with the ability to access email, Web, and other Internet applications on the move. In this paper, we observe that while the mobile computing landscape has changed both in terms of number and type of hotspot venues, there are several technological and deployment challenges remaining before hotspots can ...

15 T1-A: next generation mobile networks symposium: Titan: a new paradigm in wireless internet access based on community collaboration
Bjorn Landfeldt, Jahan Hassan, Albert Y. Zomaya, Suparerk Manitpornsut, Riky Subrata
July 2006 **Proceeding of the 2006 international conference on Communications and mobile computing IWCMC '06**
Publisher: ACM Press
Full text available: pdf(206.80 KB) Additional Information: full citation, abstract, references, index terms

This paper introduces project TITAN, which investigates an alternative construct of residential broadband access. The aim of the project is to increase the utilisation of deployed broadband capacity such as xDSL and cable modem connections. In order to achieve this, we propose a Collaborative Community Network (CCN) where residential broadband users contribute their *spare* broadband capacity to other users over a wireless medium, to form a collaborative community wireless Internet access n ...

Keywords: DSL, WLAN, access network, wireless internet, wireless networks

16 Applications II: Embedding JAAS in agent roles to apply local security policies
Giacomo Cabri, Luca Ferrari, Letizia Leonardi
June 2004 **Proceedings of the 3rd international symposium on Principles and practice of programming in Java PPPJ '04**
Publisher: Trinity College Dublin
Full text available: pdf(106.63 KB) Additional Information: full citation, abstract, references, citings

Agents are an emerging technology that grants programmers a new way to exploit distributed resources. Roles are a powerful concept that can be used to model agent interactions, allowing agents to dynamically acquire operations to make specific tasks, and enabling separation of concerns and code reusability. Nevertheless roles should be developed taking into account permissions needed for the execution of their operations. The standard Java policy file mechanism does not suffice in this scenario, ...

Keywords: Java agents, authentication, local policies, roles

17 Equipping smart devices with public key signatures
Xuhua Ding, Daniele Mazzocchi, Gene Tsudik
February 2007 **ACM Transactions on Internet Technology (TOIT)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(274.64 KB) Additional Information: full citation, abstract, references, index terms

One of the major recent trends in computing has been towards so-called smart devices, such as PDAs, cell phones and sensors. Such devices tend to have a feature in common: limited computational capabilities and equally limited power, as most operate on batteries. This makes them ill-suited for public key signatures. This article explores practical and conceptual implications of using Server-Aided Signatures (SAS) for these devices. SAS is a signature method that relies on partially-trusted serve ...

Keywords: Digital signatures, public key infrastructure

18 A heterogeneous-network aided public-key management scheme for mobile ad hoc networks
Yuh-Min Tseng
January 2007 **International Journal of Network Management**, Volume 17 Issue 1
Publisher: John Wiley & Sons, Inc.
Full text available: pdf(231.50 KB) Additional Information: full citation, abstract, references, index terms

A mobile ad hoc network does not require fixed infrastructure to construct connections among nodes. Due to the particular characteristics of mobile ad hoc networks, most existing secure protocols in wired networks do not meet the security requirements for mobile ad hoc networks. Most secure protocols in mobile ad hoc networks, such as secure routing, key agreement and secure group communication protocols, assume that all nodes must have pre-shared a secret, or pre-obtained public-key certificate ...

19 Applied cryptography II: Multi-signatures in the plain public-Key model and a general forking lemma
Mihir Bellare, Gregory Neven
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(279.93 KB) Additional Information: full citation, abstract, references, index terms

A multi-signature scheme enables a group of signers to produce a compact, joint signature on a common document, and has many potential uses. However, existing schemes impose key setup or PKI requirements that make them impractical, such as requiring a dedicated, distributed key generation protocol amongst potential signers, or assuming strong, concurrent zero-knowledge proofs of knowledge of secret keys done to the CA at key registration. These requirements limit the use of the schemes. We provi ...

Keywords: cryptography, digital signatures, forking lemma, multi-signatures

20 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

Albert Levi, M. Ufuk Caglayan, Cetin K. Koc

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

pre-authenticate and public key SEARCH

Feedback Report a problem Satisfaction survey

Terms used **pre authenticate** and **public key**

Found **37,229** of **201,062**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 21 - 40 of 200 Result page: previous 1 **2** 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □ □ □ □ ■

21 Scalable public-key tracing and revoking

Yevgeniy Dodis, Nelly Fazio, Aggelos Kiayias, Moti Yung

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing PODC '03**

Publisher: ACM Press

Full text available: pdf(1.17 MB) Additional Information: full citation, abstract, references, citings, index terms

Traitor Tracing Schemes constitute a very useful tool against piracy in the context of digital content broadcast. In such multi-recipient encryption schemes, each decryption key is fingerprinted and when a pirate decoder is discovered, the authorities can trace the identities of the users that contributed in its construction (called traitors). Public-key traitor tracing schemes allow for a multitude of non trusted content providers using the same set of keys, which makes the scheme "server-side ...

Keywords: Broadcast Encryption, Digital Content Distribution, Multicast, Scalability, Traitor Tracing

22 Cryptosystems: Securely combining public-key cryptosystems

Stuart Haber, Benny Pinkas

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**

Publisher: ACM Press

Full text available: pdf(416.51 KB) Additional Information: full citation, abstract, references, citings, index terms

It is a maxim of sound computer-security practice that a cryptographic key should have only a single use. For example, an RSA key pair should be used only for public-key encryption or only for digital signatures, and not for both.In this paper we show that in many cases, the simultaneous use of related keys for two cryptosystems, e.g. for a public-key encryption system and for a public-key signature system, does not compromise their security. We demonstrate this for a variety of public-key encry ...

23 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent

October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

24 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Publisher: ACM Press

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

25 Secret key distribution protocol using public key cryptography
Amit Parnerkar, Dennis Guster, Jayantha Herath
October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

26 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(107.24 KB) Additional Information: full citation, abstract, references, index terms

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, the visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the UMTS architecture carry the heritage of the GSM's philosophy regarding the user/network authentication and the data ciphe ...

Keywords: PKIs, PLMNs, asymmetric cryptography

27 Proactive public key and signature systems
Amir Herzberg, Markus Jakobsson, Stanislław Jarecki, Hugo Krawczyk, Moti Yung
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: pdf(1.51 MB) Additional Information: full citation, references, citings, index terms

28 Trust, recommendations, evidence, and other collaboration know-how (TRECK): How to incorporate revocation status information into the trust metrics for public-key certification
Kemal Bicakci, Bruno Crispo, Andrew S. Tanenbaum
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**
Publisher: ACM Press
Full text available: pdf(124.41 KB) Additional Information: full citation, abstract, references, index terms

In a traditional PKI, the trust associated with a public key is expressed in binary either by 0 or 1. Alternatively, several authors have proposed trust metrics to evaluate the confidence afforded by a public key. However their work has a static point of view and does not take into account the issue of public key revocation. In this paper, we make the first attempt to incorporate the revocation status information into the trust metrics for public key certification. To achieve our goal, we use a ...

Keywords: PKI, public key certificates, revocation, trust metrics

29 Public-key cryptography and password protocols: the multi-user case
Maurizio Kliban Boyarsky
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

30 Advances in public-key certificate standards
Warwick Ford
July 1995 **ACM SIGSAC Review**, Volume 13 Issue 3
Publisher: ACM Press
Full text available: pdf(556.65 KB) Additional Information: full citation, abstract, references, citings, index terms

To build effective public-key infrastructures, well-entrenched standards are essential because many different applications and different vendor products need to be supported and used. Standards for public-key certificate and certificate revocation list (CRL) formats are most important. The recognized standard in this area is ITU-T X.509, first published in 1988. In 1993, the Internet Privacy Enhanced Mail (PEM) proposals refined the use of X.509. However, more recently it has become apparent tha ...

31 Issues 94—public key—trials and tribulations
Harvey H. Rubinovitz
July 1995 **ACM SIGSAC Review**, Volume 13 Issue 3
Publisher: ACM Press
Full text available: pdf(297.30 KB) Additional Information: full citation, abstract, references, index terms

This document was written based on the introductory talk presented at the special workshop, "Issue 94 - Public Key - Trials and Tribulations" in conjunction with the Tenth Annual Computer Security Applications Conference held in December 1994. This document serves to set the stage for the papers which follow and to provide a catalyst to discussions at the conference. Applications which utilize public key technology to enhance security are just starting to emerge. Some applications are starting t ...

32 Applied cryptography II: Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation
Mihir Bellare, Tadayoshi Kohno, Victor Shoup
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(235.26 KB) Additional Information: full citation, abstract, references, index terms

We show how to significantly speed-up the encryption portion of some public-key cryptosystems by the simple expedient of allowing a sender to maintain state that is re-used across different encryptions.In particular we present stateful versions of the DHIES and Kurosawa-Desmedt schemes that each use only 1 exponentiation to encrypt, as opposed to 2 and 3 respectively in the original schemes, yielding the fastest discrete-log based public-key encryption schemes known in the random-oracle and stan ...

Keywords: cryptography, public-key encryption

33 Identification control: Public key distribution through "cryptoIDs"
Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press
Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

34 Public-key support for group collaboration
Carl Ellison, Steve Dohrmann
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(561.61 KB) Additional Information: full citation, abstract, references, index terms

This paper characterizes the security of group collaboration as being a product not merely of cryptographic algorithms and coding practices, but also of the man-machine process of group creation. We show that traditional security mechanisms do not properly address the needs of a secured collaboration and present a research prototype, called NGC (next generation collaboration), that was designed to meet those needs. NGC distinguishes itself in the care with which the man-machine process was analy ...

Keywords: Human-computer interface, IPsec, PGP, PKI, S/MIME, SDSI, SPKI, SSH

35 An authorization model for a public key management service
Pierangela Samarati, Michael K. Reiter, Sushil Jajodia
November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(337.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Public key management has received considerable attention from both the research and commercial communities as a useful primitive for secure electronic commerce and secure communication. While the mechanics of certifying and revoking public keys and escrowing and recovering private keys have been widely explored, less attention has been paid to access control frameworks for regulating access to stored keys by different parties. In this article we propose such a framework for a key management ser ...

Keywords: Access control, authorizations specification and enforcement, public key infrastructure

36 A public-key based secure mobile IP
John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra
September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking MobiCom '97**
Publisher: ACM Press
Full text available: pdf(1.95 MB) Additional Information: full citation, references, citings

37 Is hierarchical public-key certification the next target for hackers?
Mike Burmester, Yvo G. Desmedt
August 2004 **Communications of the ACM**, Volume 47 Issue 8
Publisher: ACM Press
Full text available: pdf(173.38 KB) html(27.53 KB) Additional Information: full citation, abstract, references, citings, index terms

Considering alternatives to hierarchical authentication structures that are not sufficiently secure for communication on open networks such as the Internet.

38 Public-key cryptosystems provably secure against chosen ciphertext attacks
M. Naor, M. Yung
April 1990 **Proceedings of the twenty-second annual ACM symposium on Theory of**

computing STOC '90

Publisher: ACM Press

Full text available: pdf(1.10 MB) Additional Information: full citation, citings, index terms

39 Which PKI (public key infrastructure) is the right one? (panel session)

Carlisle Adams, Mike Burmester, Yvo Desmedt, Mike Reiter, Philip Zimmermann

November 2000 **Proceedings of the 7th ACM conference on Computer and communications security CCS '00**

Publisher: ACM Press

Full text available: pdf(207.61 KB) Additional Information: full citation, references, index terms

40 Key establishment in sensor networks: TinyPK: securing sensor networks with public key technology

Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, Peter Kruus

October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks SASN '04**

Publisher: ACM Press

Full text available: pdf(204.55 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless networks of miniaturized, low-power sensor/actuator devices are poised to become widely used in commercial and military environments. The communication security problems for these networks are exacerbated by the limited power and energy of the sensor devices. In this paper, we describe the design and implementation of public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks. Our work ...

Keywords: TinyOS, authentication, cryptography, diffie-hellman, encryption, key management, public key (PK), rivest shamir adelman (RSA), sensor networks

Results 21 - 40 of 200 Result page: previous 1 **2** 3 4 5 6 7 8 9 10 next

Web Images Video News Maps Gmail more ▾ Sign in

Google

public key and pre-authentication [Search] Advanced Search Preferences

The **"AND"** operator is unnecessary -- we include all search terms by default. [details]

Web Results **1** - **10** of about **46,900** for **public key and pre-authentication**. (**0.25** seconds)

draft ietf cat kerberos pk recovery 01 txt
The two main issues for recovery are updating the KDC **public key** with all ... secret **key** K2 encrypted in Diffie-Hellman shared secret **key**) **preauthentication** ...
www3.ietf.org/proceedings/98dec/I-D/draft-ietf-cat-kerberos-pk-recovery-01.txt - 20k -
Cached - Similar pages

> 00
> The Extension The following new **preauthentication** type is proposed: PA-EXTRA-TGT 22 The ... **Public Key** Cryptography for Initial Authentication in Kerberos. ...
> www3.ietf.org/proceedings/98dec/I-D/draft-ietf-cat-kerberos-extra-tgt-00.txt - 8k -
> Cached - Similar pages
> [More results from www3.ietf.org]

RFC 4557 Online Certificate Status Protocol (OCSP) Support for ...
Message Definition A **pre-authentication** type identifier is defined for this ... [RFC4556] Zhu, L. and B. Tung, "**Public Key** Cryptography for Initial ...
tools.ietf.org/html/rfc4557 - 22k - Cached - Similar pages

> draft-ietf-cat-kerberos-pk-init-22 - **Public Key** Cryptography for ...
> Conversely, **public-key** cryptography (in conjunction with an established ... use of the following new **preauthentication** types: PA-PK-AS-REQ 16 PA-PK-AS-REP ...
> tools.ietf.org/html/draft-ietf-cat-kerberos-pk-init-22 - 81k - Cached - Similar pages
> [More results from tools.ietf.org]

Protocol Action: '**Public Key** Cryptography for Initial ...
These extensions provide a method for integrating **public key** cryptography into ... signature and/or encryption algorithms in **pre-authentication** data fields. ...
www1.ietf.org/mail-archive/web/ietf-announce/current/msg02221.html - 9k -
Cached - Similar pages

Online Certificate Status Protocol (OCSP) Support for **Public Key** ...
There is no binding between PA-PK-OCSP-RESPONSE **pre-authentication** data and PKINIT ... [RFC4556] Zhu, L. and B. Tung, "**Public Key** Cryptography for Initial ...
www.rfc-zone.org/rfc4557.html - 21k - Cached - Similar pages

[PS] **PUBLIC-KEY** LOGIN FOR DCE 1.2
File Format: Adobe PostScript - View as Text
PARTY **pre-authentication** field attached to a request for a **public-key** user login will provide proof to the login-. agent that the system requesting the ...
www.opengroup.org/tech/rfc/mirror-rfc/rfc68.0.ps - Similar pages

rfc 4556
These extensions provide a method for integrating **public key** ... obtain the encryption **key** for decrypting the KDC reply is returned in a **pre- authentication** ...
www.ietf.org/rfc/rfc4556.txt - 99k - Cached - Similar pages

Sesame Authentication protocol 1. Abstract This document defines ...
If **public key** cryptography is used, **public key** data is transported in **preauthentication** data fields to help establish identity. 4.1. ...
srg.cs.uiuc.edu/Security/nephilim/Internal/SESAME.txt - 18k -
Cached - Similar pages

Logging on with a Smart Card
The Kerberos SSP on the client computer sends the user's **public key** certificate to the KDC as **preauthentication** data in its initial authentication request, ...
www.microsoft.com/technet/prodtechnol/

Web Images Video News Maps Gmail more ▾ Sign in

Google

public key and pre-authentication Search Advanced Search Preferences

The **"AND"** operator is unnecessary -- we include all search terms by default. [details]

Web Results **11** - **20** of about **46,900** for **public key and pre-authentication**. (**0.26** seconds)

PK_INIT Home Page
Public key cryptography makes it easier to scale **key** distribution and management. ... Standard PK_INIT: The random **key** is sent back in a **preauthentication** ...
gost.isi.edu/info/pk_init/ - 3k - Cached - Similar pages

Windows IT Pro Logo Home | Books | Chapters | Topics | Authors ...
When logging on using a smart card, the **preauthentication** data consist of a signature and the user's **public key** certificate. ...
www.windowsitlibrary.com/Content/617/06/6.html - Similar pages

SRP: Competitive Analysis
A site that uses SRP authentication with SSH can use ad-hoc **public-key** distribution, ... The default form of **preauthentication** Kerberos V5 is an encrypted ...
srp.stanford.edu/analysis.html - 15k - Cached - Similar pages

[PS] DCE 1.2.2 **PUBLIC KEY** LOGIN — FUNCTIONAL SPECIFICATION
File Format: Adobe PostScript - View as Text
If the KDC is unable to authenticate the user with the supplied **public key pre-authentication** data, the KDC returns. error information. ...
www.opengroup.org/tech/rfc/mirror-rfc/rfc68.2.ps - Similar pages

RFC 4557
There is no binding between PA-PK-OCSP-RESPONSE **pre-authentication** data and ... Previous: RFC 4556 - **Public Key** Cryptography for Initial Authentication in ...
www.faqs.org/rfcs/rfc4557.html - 14k - Cached - Similar pages

draft zhu pku2u 01 txt
Abstract This document defines the **public key** cryptography based user-to-user ... The initiator always includes the PA_PK_AS_REQ **pre-authentication** data ...
www.ietf.org/internet-drafts/draft-zhu-pku2u-01.txt - 22k - Cached - Similar pages

RFC 4556 **Public Key** Cryptography for Initial Authentication in ...
These extensions provide a method for integrating **public key** ... PKINIT **Pre-authentication** Syntax and Use This section defines the syntax and use of the ...
www1.tools.ietf.org/html/rfc4556 - 132k - Cached - Similar pages

> draft-ietf-cat-kerberos-pk-init-28 - **Public Key** Cryptography for ...
> PKINIT **Pre-authentication** Syntax and Use This section defines the syntax and use ... Using **Public Key** Encryption In this case, the PA-PK-AS-REP contains a ...
> www1.tools.ietf.org/html/draft-ietf-cat-kerberos-pk-init-28 - 147k - Cached - Similar pages

[PDF] E&CE 710 Topic 4 Sequence Design and Cryptography, Fall 2005
File Format: PDF/Adobe Acrobat - View as HTML
Key distribution, management and certification – **public-key** approach: **pre-authentication**,. authenticators for unauthenticated model, **key** transport and **key** ...
www.cacr.math.uwaterloo.ca/gradstudies/sequences.pdf - Similar pages

[PPT] NIST PKI06: Integrating PKI and Kerberos
File Format: Microsoft Powerpoint - View as HTML
The AS-REQ may optionally contain **pre-authentication** data to prove the client's ... Establishment of Kerberos Cross Realm relationships using **Public Key** ...
middleware.internet2.edu/pki06/proceedings/altman-**public_key**_kerberos.ppt - Similar pages

Web Images Video News Maps Gmail more ▾ Sign in

Google

public key and pre-authentication | Search | Advanced Search
Preferences

The **"AND"** operator is unnecessary -- we include all search terms by default. [details]

Web Results **21** - **30** of about **46,900** for **public key and pre-authentication**. (**0.09** seconds)

[rfc-dist] RFC 4556 on **Public Key** Cryptography for Initial ...
RFC 4556 Title: **Public Key** Cryptography for Initial Authentication in Kerberos (PKINIT) ... and/or encryption algorithms in **pre-authentication** data fields. ...
www.postel.org/pipermail/rfc-dist/2006-June/001299.html - 7k -
Cached - Similar pages

draft-ietf-cat-kerberos-pk-init-30 - **Public Key** Cryptography for ...
PKINIT **Pre-authentication** Syntax and Use This section defines the syntax and use ... Using **Public Key** Encryption In this case, the PA-PK-AS-REP contains an ...
www3.tools.ietf.org/html/draft-ietf-cat-kerberos-pk-init-30 - 179k -
Cached - Similar pages

[PDF] Talking to Strangers
File Format: PDF/Adobe Acrobat - View as HTML
Public Key Cryptography. • **Pre-Authentication**. 4/11/2003. Erkang Zheng. 6. Computer Science. Location-Limited Channels. • Used for **Pre-Authentication** ...
discovery.csc.ncsu.edu/Courses/csc774-S03/Presentations/14-Talk2Strangers.pdf -
Similar pages

Roger Clarke's 'Authentication Revisited'
Authentication Re-visited: How **Public Key** Infrastructure Could Yet Prosper ... 'out of band' **pre-authentication** of the association between a **key**-pair and an ...
www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html - 57k -
Cached - Similar pages

[PDF] **PRE-AUTHENTICATION** USING INFRARED
File Format: PDF/Adobe Acrobat
information for its first phase, the so called **pre-authentication** phase. ... example a **public key**). This may be done not only by direct com- ...
www.springerlink.com/index/j3347570x1087128.pdf - Similar pages

kerb pkinit html
In PKINIT, the first message contains additional information in the **pre-authentication** field: The **public key** of U, a timestamp, the nonce repeated, ...
www.avispa-project.org/library/Kerb-PKINIT.html - 10k - Cached - Similar pages

[PDF] AN EFFICIENT SIM-BASED AUTHENTICATION AND **KEY** DISTRIBUTION METHOD ...
File Format: PDF/Adobe Acrobat
The MH starts a **pre-authentication** request. In the. message, it provides the current AP's SSID and session ID as. this AP's **public key**. ...
ieeexplore.ieee.org/iel5/10384/33117/01557185.pdf?arnumber=1557185 -
Similar pages

[PPT] Talking to Strangers: Authentication in Ad-Hoc Wireless Networks
File Format: Microsoft Powerpoint - View as HTML
Exchanging the commitment of **public key** information. (**Preauthentication**). Doing Common Authentication Procedure (SSL, IKEKE). Two-Party Protocols(1/5) ...
camars.kaist.ac.kr/~hyoon/courses/cs710_2002_fall/2002cas/security/tp/%5BS10%5D.ppt - Similar pages

[PDF] **PRE-AUTHENTICATION** USING INFRARED
File Format: PDF/Adobe Acrobat - View as HTML
Pre-authentication: Secure establishment of a shared secret or mutual knowledge. of identifying data about the other device (for example a **public key**). ...
www.vs.inf.ethz.ch/events/sppc04/papers/sppc04_spahic.pdf - Similar pages

[PDF] Network Working Group L. Zhu
File Format: PDF/Adobe Acrobat - View as HTML
the validity of the certificates used in **Public Key** Cryptography for ... A **pre-authentication** type identifier is defined for this mechanism: ...
ietfreport.isoc.org/rfc/PDF/rfc4557.pdf - Similar pages

Previous 1 2 3 4 5 6 7 8 9 10 11 12 **Next**

public key and pre-authentication Search

Search within results | Language Tools | Search Tips